tests, and in-store video surveillance. The difference, Lane argues, between these old methods of data gathering and electronic surveillance involves quantity:

Technology makes it possible for employers to gather enormous amounts of data about employees, often far beyond what is necessary to satisfy safety or productivity concerns. And the trends that drive technology—faster, smaller, cheaper—make it possible for larger and larger numbers of employers to gather ever-greater amounts of personal data. (3-4)

Lane points out that employers can collect data whenever employees use their computers—for example, when they send e-mail, surf the Web, or even arrive at or depart from their workstations.

Another key difference between traditional surveillance and electronic surveillance is that employers can monitor workers’ computer use secretly. One popular monitoring method is keystroke logging, which is done by means of an undetectable program on employees’ computers. The Web site of a vendor for Spector Pro, a popular keystroke logging program, explains that the software can be installed to operate in “Stealth” mode so that it “does not show up as an icon, does not appear in the Windows system tray, . . . [and] cannot be uninstalled without the Spector Pro password which YOU specify” (“Automatically”). As Lane explains, these programs record every key entered into the computer in hidden directories that can later be accessed or uploaded by supervisors; the programs can even scan for keywords tailored to individual companies (128-29).